Virtual Private Networks, 2nd Edition
By Mike Erwin, Charlie Scott, Paul Wolfe

Table of Contents

Chapter 4. Implementing Layer 2 Connections

4.1 Differences Between PPTP, L2F, and L2TP

Both PPTP and L2F allow you to use any authentication method you would normally use with PPP, including PAP and CHAP—essentially whatever authentication protocols both the client and server support. For encryption, PPTP uses the RC4 cipher with either 40-bit or 128-bit keys. L2F, on the other hand, supports 40-bit or 56-bit DES encryption with the 11.2 versions of Cisco's IOS. IOS version 11.3(3)T and later supports IPSec, which can also be used to encrypt an L2F connection.

L2TP combines the best features of PPTP and L2F and allows for either client-initiated or remote access switch-initiated L2TP connections. You can use L2TP in any situation where you might use PPTP or L2F. It can still use the same authentication protocols as the others, including PAP, CHAP, and MS-CHAP. IPSec is the recommended encryption mechanism for L2TP. Although that L2TP was reputed to "replace" PPTP, Microsoft has chosen to continue providing PPTP in Windows NT 5.0 for those who do not wish to maintain the public key infrastructure required for IPSec.

PPTP is available on currently shipping versions of Windows NT Server 4.0 and Windows NT Workstation 4.0 as part of Remote Access Services (RAS)—NT's dial- up networking software. Microsoft's PPTP support for Windows 95 is included in their Dial-Up Networking Upgrade Version 1.3. Microsoft has also released LAN-to-LAN PPTP connections for Windows NT in their "Routing and Remote Access" software (codenamed "Stronghold"), as part of the Windows NT Option Pack. PPTP support is included in Windows 98. Microsoft Windows NT 5.0 will also support PPTP connections.

A Macintosh PPTP client is available from Network TeleSystems (http://www.nts.com). Called TunnelBuilder, it offers full PPTP support, including NT domain login and data encryption. Network TeleSystems (NTS) also has a version of TunnelBuilder for Windows 95, Windows 98, Windows for Workgroups, and Windows 3.1. Since Microsoft doesn't plan on supporting PPTP on down-level versions of Windows, this allows users with legacy systems to run PPTP. The NTS Windows clients support L2TP. In addition, Linux is now capable of supporting PPTP.

There are also a number of hardware devices that support PPTP out of the box. These devices are known variously as remote access servers, remote hubs, terminal servers, and remote access switches. In this chapter, we will refer to them simply as remote access switches, because that term is prevalent in the industry and best describes what they do. There are a number of remote access switches that support PPTP, among them Ascend's MAX line, the 3Com/U.S. Robotics Total Control line, and ECI Telematics' Nevada. These are typical brands used in ISP points-of-presence and corporate networks to terminate modem and ISDN calls. PPTP is included as part of all of these products free of charge—no additional activation fees are required. There are also some hardware devices that act as PPTP servers, but do not operate as a standard remote access

switch. Examples of these are the Bay Networks Extranet Switch and the NTS TunnelMaster.

L2F is supported by Cisco in their IOS software for their routers. Other vendors, such as Nortel and Shiva, also support L2F. L2TP is supported in Cisco IOS 11.3(5)AA and later. In addition, many other hardware devices support it. Microsoft will include L2TP support in Windows NT 5.0. Because PPTP, L2F, and L2TP operate similarly, we will concentrate on PPTP and L2TP.